Clinical system security: interim guidelines

Ross Anderson

The BMA asked Ross Anderson to draw up interim guidelines on maintaining security in computerised patient information systems. We publish them here together with the principles on which they are based. The guidelines are designed to help clinicians avoid the most common serious mistakes in computer security and are being published to stimulate discussion of the issues. The principles are discussed fully in "Security in Clinical Information Systems," which is available from the BMA (Dr Fleur Fisher, Department of Ethics, Science, and Information).

Recent articles have illustrated several threats to the confidentiality of personal health information. Many medical records can be easily obtained by private detectives, who typically telephone a general practice, family health services authority, or hospital and pretend to be the secretary of a doctor giving emergency treatment to the person who is the subject of the investigation. One article found that most patients' personal health information could be compromised in this way and was routinely sold by agencies for as little as £150.[1,2] Nationwide health networking is also seen as a further threat to confidentiality because health records will be available to many more people. These interim guidelines have therefore been drawn up to help tackle the pressing short term concerns; they are supplementary to existing documentation such as *The Handbook of Information Security*.[3]

Careless disclosure

The main threat to the confidentiality of clinical records is carelessness about telephone inquiries of the kind described above. This threat may be largely eliminated if staff follow a number of common sense rules that the best practices have used for years and that are now agreed by the NHS Executive. Whether records are computerised or not, these rules of best practice can be summed up as: clinician-consent-call back-care-commit:

- only a clinician should release personal health information. It should not be released by a receptionist or secretary;
- the patient's consent must be obtained, except when the patient is known to be receiving treatment from the caller or in the case of emergency or the statutory exemptions. In the latter two cases the patient must be notified as soon as reasonably possible afterwards;
- the clinician must call back if the caller is not known personally—and the number must be verified—for example, in the Medical Directory. This procedure must be followed even when an emergency is claimed, as private investigators routinely claim emergencies;
- care must be taken, especially when the information is or may be highly sensitive, such as HIV status, details of contraception, psychiatric history, or any information about celebrities;
- the clinician must commit a record of the disclosure to a ledger. This should have the patient's name; whether consent was sought at the time (and, if not, the date and means of notification); the number called back and how it was verified; and whether anything highly sensitive was disclosed.

Telephone calls that aim to get information on a false pretext are not unique to medicine: they are also widely used in industrial espionage, whether to obtain information directly or to get passwords for computer systems.[4] Experienced investigators will be convincing, so it is important to have rules that are always followed. People often ask whether personal health information may be sent by fax. It is prudent, and it is the BMA's established advice, that personal health information should be faxed only to a machine that is known to be secure during working hours.[5] In addition, the guidelines for disclosures by telephone should also apply to faxes. Verifying the identity or, failing that, the location of the caller is just as important as it is when disclosing personal health information over the telephone.

Equipment theft, loss, and damage

The most serious threat to the continued availability of computerised clinical information in general practice is theft of the computer; this has been experienced by over 10% of general practices surveyed.[6] Data can also be destroyed in other ways such as by fire, flood, equipment failure, and computer viruses. Physical security measures must be taken, as well as hygiene rules to control the risk of computer virus infestation. But even if these were completely effective (which they never are), the risk of equipment failure still makes it essential to have a tested recovery plan.

Unfortunately, most organisations do not perform realistic tests of their procedures, with the result that when real disasters strike recovery is usually held up for lack of manuals, suppliers' phone numbers, and other things whose criticality had simply not been foreseen. It is thus prudent to have a drill based on a realistic scenario, such as the complete destruction of a surgery or hospital computer room by fire, and to perform a full system recovery to another machine from back up media held off site.

Keeping several generations of back ups is also prudent, since with equipment failure and with some viruses it may take time to notice that something has gone wrong. A typical schedule in a well run establishment might involve back ups aged one, two, three, four, eight, and twelve weeks, as well as daily incremental back ups.

Access control

A serious threat to the confidentiality of personal health information in hospitals and health authorities is the poor design and lax administration of access controls.[7,8] In many hospitals all users may access all records; users also often share passwords and leave terminals permanently logged on for the use of everyone in a ward. Such behaviour causes a breakdown of clinical and medicolegal accountability and may lead to direct harm: one case has been reported in which a psychiatric patient changed prescription information at a terminal that was left logged on.

The introduction of networking may turn local vulnerabilities into global ones. If systems with ineffective access controls are connected together in a network then instead of the data being available merely

Computer Laboratory, University of Cambridge, Cambridge CB2 3QG
Ross Anderson, *lecturer*

BMJ 1996;312:109-11

to all staff in the hospital they might become available to everyone on the network.

Effective access controls are thus a prerequisite for networking. Access controls must also be harmonised among networked systems, or moving information from one system to another could result in leaks. The basis for this should be a common security policy that says who may access what records, under what circumstances. To facilitate clinical computer networking, the BMA has developed such a security policy[9]; its principles are listed in the box. Until there is agreement on a common security policy connecting clinical systems to the NHS wide network is not advised.

Meanwhile much can be achieved to control local threats by careful management of existing access controls. It is prudent, for example, to cover the following points.

- A senior person such as a hospital manager or partner in general practice must be responsible for security, especially if routine administration is delegated to junior staff. Many security failures result from delegating responsibility to people without the authority to insist on good practice.
- The mechanisms for identifying and authenticating users should be managed carefully. For example, users should be educated to pick passwords that are hard to guess and to change them regularly; and terminals should be logged off automatically after being unused for five minutes.
- Systems should be configured intelligently. Dangerous defaults such as maintenance passwords and anonymous file transfer access supplied by the manufacturer should be removed. User access should be restricted to departments or care teams as appropriate. With hospital systems that hold records on many people, only a few staff should have access to the files of patients not currently receiving treatment.
- Periodic audits should be carried out, and from time to time these should include penetration tests. A private detective might, for example, be paid to obtain the personal health information of a consenting patient. In this way, any channels that have developed to sell information on the black market may be identified and closed off.

Communications security: dial access

Some general practices have branch surgeries, and many hospitals have branch clinics, so the possibility of access via a dial up modem from branches is often raised. In such cases, the main additional risk is that an outside hacker might dial up the main system and gain access by guessing a password. So the following would be good practice.

- There should be no direct dial access to the main computer system. Instead the main system should dial back the branches.
- Extra effort should be made to educate users to choose passwords with care, and all incidents should be investigated diligently.

Great care should be taken when any form of dial in access to a clinical system is permitted. This is occasionally convenient for system maintenance; in such cases it is prudent to enable the modem to receive an incoming call only after arranging the service call by telephone. Maintenance passwords should be changed from their original default values to fresh ones and should also be changed after every maintenance call.

Communications security: wide area networks

A growing number of clinicians transfer personal health information using electronic mail across wide area networks. Examples are the mailbox systems that general practitioners use to transfer registration data and item of service claims to family health services authorities, links between general practitioners and hospitals for pathology reports, and the use of Internet electronic mail to communicate with patients with chronic conditions that require continuing management.

Exactly the same principles apply to email as to telephones and faxes. With wide area networks, however, messages may pass through a number of untrusted computers en route, so it is difficult to obtain guarantees about who might receive or who might have transmitted a given message.

This problem may be tackled using cryptography: encryption and digital signatures can protect personal health information against disclosure and alteration, whether accidental or malicious, while in transit through a network. Standards for encryption and digital signatures are the subject of current European standards initiatives and efforts by the NHS Executive. Until then the encryption program PGP (Pretty Good Privacy) may be used. This is available free for most common makes of computer and is adequate (though not ideal). Until there are more definitive standards the careful use of PGP is recommended, and suggestions for interfacing it to access control systems may be found in *Security in Clinical Information Systems*, available from the BMA.[9]

Protection of messages is not the only concern, however. When clinical systems are attached to wide area networks the risk arises that an attacker might use the network to penetrate the system. Attacks by outsiders are much rarer than those by insiders, but they still happen from time to time.

Many doctors who use the Internet at present do so from home computers rather than from equipment in their clinic or office. Before they connect systems that contain personal health information to wide area networks they should study the risks. There is a standard book on wide area network security by Cheswick and Bellovin.[10]

As noted above, systems with weak access controls are particularly at risk from outside attack. The risk can be mitigated by the use of "firewalls"—machines that filter traffic and block the better known technical attacks. There are, however, no panaceas, especially if a number of systems share the same firewall, as users of all these systems might still be able to access each other's information. In any case, reliance on the firewall facilities of the NHS wide network is not advised, as the NHS Executive has refused to allow the BMA to inspect them.

Disclosure to third parties

Third parties such as social workers, policemen, and lawyers may get access to personal health information, whether with the patient's consent or via statutory provisions for disclosure. Personal health care information should not be provided electronically to such outside bodies but given in paper form. Apart from the difficulty of assessing the security of third parties' computer systems, raw electronic access is of little evidential value.

Both the Civil Evidence Act and the Police and Criminal Evidence Act require that for computer evidence to be admissible there must be a certificate from the operator of the computer. There are also practical problems with explaining Read and other codes and preventing the accidental disclosure of information to which the recipient is not entitled. A letter containing information abstracted from the record keeping system is thus safer, simpler, and more able to satisfy a requirement for evidence.

Nine principles of data security

(1) **Access control**—Each identifiable clinical record shall be marked with an access control list naming the people or groups of people who may read it and append data to it. The system shall prevent anyone not on the list from accessing the record in any way.

(2) **Record opening**—A clinician may open a record with herself and the patient on the access control list. When a patient has been referred she may open a record with herself, the patient, and the referring clinician(s) on the access control list.

(3) **Control**—One of the clinicians on the access control list must be marked as being responsible. Only she may change the access control list and she may add only other health care professionals to it.

(4) **Consent and notification**—The responsible clinician must notify the patient of the names on his record's access control list when it is opened, of all subsequent additions, and whenever responsibility is transferred. His consent must also be obtained, except in emergency or in the case of statutory exemptions.

(5) **Persistence**—No one shall have the ability to delete clinical information until the appropriate time has expired.

(6) **Attribution**—All accesses to clinical records shall be marked on the record with the name of the person accessing the record as well as the date and time. An audit trail must be kept of all deletions.

(7) **Information flow**—Information derived from record A may be appended to record B if and only if B's access control list is contained in A's.

(8) **Aggregation control**—Effective measures should exist to prevent the aggregation of personal health information. In particular, patients must receive special notification if any person whom it is proposed to add to their access control list already has access to personal health information on a large number of people.

(9) **Trusted computing base**—Computer systems that handle personal health information shall have a subsystem that enforces the above principles in an effective way. Its effectiveness shall be evaluated by independent experts.

The dispute over the NHS-wide network

Two shortcomings of the proposed NHS wide network have already been discussed: the absence of an agreed common security policy enforced by all the systems that will connect to it and lack of confidence in the technical security measures such as firewalls.

A third and equally serious objection is that many of the applications that the NHS wide network has been designed to support are ethically objectionable in that they will make personal health information available to an ever growing number of administrators and others outside the control of both patient and clinician. Such availability contravenes the ethical principle that personal health information may be shared only with the patient's informed and voluntary consent.[5]

A growing number of administrative systems fall into this category. For example, the administrative registers will record patients' use of contraceptive and mental health services, while the NHS clearing system will handle contract claims for inpatient hospital treatment and contain a large amount of identifiable clinical information. According to the NHS Executive pressure will be applied to clinicians to persuade them to send data to the clearing system over the NHS wide network. The BMA therefore requested access to conduct an independent security review; the NHS Executive has so far refused.

Another problem is item of service and other information sent over existing electronic links between general practitioners and family health services authorities. While registration links are fairly innocuous, at least two suppliers are developing software for authorities which enables claims for items of service, prescriptions, and contract data to be pieced together into a "shadow" patient record that is outside clinical control (Advanced information system, Family Health Services computer unit, 1995; Data Logic product information at http://www.datlog.co.uk/)

The systems mentioned above are part of the strategy being pursued by the NHS Executive's information management group, whose goals include an electronic patient record that is entirely shared throughout the NHS. The collection of general practice data is understood to be the driving force and general practice systems will be interrogated remotely by the NHS. These goals are in clear conflict with the ethical position of the BMA.[5] They also contravene the guidance from the joint computer group of the General Medical Services Committee of the BMA and the Royal College of General Practitioners that no patient should be identifiable, other than to the general practitioner, from any data sent to an external organisation without the informed consent of the patient.[11] From the point of view of consent, a survey has shown that most patients are unwilling to share personal health information with NHS administrators.[12]

In view of these conflicts, and of the risk that creating large aggregates of personal health information will promote the kind of abuses common in the United States,[13,14] the BMA's position remains that exposing personal health information to the NHS wide network is unethical.

BMA security policy principles

In addition to the guidelines the BMA commissioned the development of a clinical information security policy.[9] This sets out nine principles designed to uphold the principle of patient consent and to be independent of the details of specific equipment. The principles (see box) provide both the philosophical basis for the guidelines and some practical reassurance. A clinician who keeps personal health information on a system that enforces these principles or sends it between such systems may have a reasonable expectation that the record will not end up being leaked.

1 Luck N, Burns J. Your secrets for sale. *Daily Express* 1994;Feb 16:p32,col 3.
2 Rogers L, Leppard D. For sale: your secret medical record for £150. *Sunday Times* 1995;Nov 26:1-2.
3 NHS Executive. *The handbook of information security.* Leeds: NHS Executive, 1995 (E5209).
4 Winkler B, Dealy B. Information security technology? Don't rely on it. A case study in social engineering. *Proceedings of the Ninth Usenix Security Symposium.*
5 Sommerville A. *Medical ethics today: its practice and philosophy.* London: BMA, 1993.
6 Pitchford RA, Kay S. GP practice computer security survey. *Journal of Informatics in Primary Care* 1995;6 Sep:12.
7 Audit Commission. *Setting the records straight: a study of hospital medical records.* London: Audit Commission, 1995.
8 Audit Commmission. *For your information: a study of information management and systems in the acute hospital.* London: Audit Commission, 1995.
9 Anderson RJ. *Security in clinical information systems.* London: BMA,1996. (also available from http://www.cl.cam.ac.uk/users/rja14 Med)
10 Cheswick WR, Bellovin SM. *Firewalls and internet security: repelling the wily hacker.* New York: Addison-Wesley, 1994.
11 Committee on Standards of Data Extraction from General Practice Guidelines, Joint Computer Group of the GMSC and RCGP. *Report.* Appendix 3. London, BMA and RCGP, 1988.
12 Hawker A. Confidentiality of personal information: a patient survey. *Journal of Informatics in Primary Care* 1995;16 Mar:19.
13 Anderson RJ. NHS wide networking and patient confidentiality. *BMJ* 1995;310:5-6.
14 Woodward B. The computer-based patient record and confidentiality. *N Engl J Med* 1995;21:141-2.